

REPORT DOCUMENTATION PAGE*Form Approved*
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Service, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY) AUGUST 2010		2. REPORT TYPE Conference Paper		3. DATES COVERED (From - To) May 2008 – May 2010	
4. TITLE AND SUBTITLE ATTACKER DETECTION GAME IN WIRELESS NETWORKS WITH CHANNEL UNCERTAINTY				5a. CONTRACT NUMBER In House	
				5b. GRANT NUMBER N/A	
				5c. PROGRAM ELEMENT NUMBER 62702F	
6. AUTHOR(S) Wenjing Wang, Mainak Chatterjee, and Kevin Kwiat				5d. PROJECT NUMBER 23G4	
				5e. TASK NUMBER IH	
				5f. WORK UNIT NUMBER 01	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AFRL/RIGG University of Central Florida 525 Brooks Road Department of Electrical Engineering and Computer Science Rome NY 13441-4505 Orlando, FL 32816				8. PERFORMING ORGANIZATION REPORT NUMBER N/A	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) AFRL/RIGG 525 Brooks Road Rome NY 13441-4505				10. SPONSOR/MONITOR'S ACRONYM(S) N/A	
				11. SPONSORING/MONITORING AGENCY REPORT NUMBER AFRL-RI-RS-TP-2010-30	
12. DISTRIBUTION AVAILABILITY STATEMENT Approved For Public Release; Distribution Unlimited. PA #: 88ABW-2009-4436 Date Cleared: 22-Oct-2009					
13. SUPPLEMENTARY NOTES © 2010 IEEE. This paper was published in the Proceedings of the 2010 IEEE International Conference of Communications. This work is copyrighted. One or more of the authors is a U.S. Government employee working within the scope of their Government job; therefore, the U.S. Government is joint owner of the work and has the right to copy, distribute, and use the work. All other rights are reserved by the copyright owner.					
14. ABSTRACT Identification and isolation of attackers in a distributed system is a challenging problem. This problem is even more aggravated in a wireless network because the unreliable channel makes the actions of the users (nodes) hidden from each other. Therefore, legitimate users can only construct a belief about a potential attacker through monitoring and observation. This work applies game theory to study the interactions between regular and attacker nodes in a wireless network. The attacker node detection process is modeled as a Bayesian game with imperfect information and it is shown that a mixed strategy perfect Bayesian Nash Equilibrium is attainable.					
15. SUBJECT TERMS Wireless Networks, Game Theory, Attack Detection					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 6	19a. NAME OF RESPONSIBLE PERSON Kevin A. Kwiat
a. REPORT U	b. ABSTRACT U	c. THIS PAGE U			19b. TELEPHONE NUMBER (Include area code) N/A

POSTPRINT

Attacker Detection Game in Wireless Networks with Channel Uncertainty

Wenjing Wang and Mainak Chatterjee
Electrical Engineering and Computer Science
University of Central Florida
Orlando, FL 32816
{wenjing, mainak}@eecs.ucf.edu

Kevin Kwiat
Information Directorate
Air Force Research Laboratory
Rome, NY 13441
kevin.kwiat@rl.af.mil

Abstract—Identification and isolation of attackers in a distributed system is a challenging problem. This problem is even more aggravated in a wireless network because the unreliable channel makes the actions of the users (nodes) hidden from each other. Therefore, legitimate users can only construct a belief about a potential attacker through monitoring and observation. In this paper, we use game theory to study the interactions between regular and attacker nodes in a wireless network. We model the attacker node detection process as a Bayesian game with imperfect information and show that a mixed strategy perfect Bayesian Nash Equilibrium is attainable. Further, we show how an attacker node can construct a nested belief system to predict the belief held by a regular node. By employing the nested belief system, a Markov Perfect Bayes-Nash Equilibrium is reached and the equilibrium postpones the detection of the attacker node. Simulation results and their discussions are provided to illustrate the properties of the derived equilibria.

I. INTRODUCTION

In a wireless network, the entities (nodes) in the network require direct and/or indirect data exchange via the network, thus it is of great importance to ensure communication security, data integrity, and information fidelity. Although advanced cryptographic techniques can be employed, the security challenges, e.g., DoS attacks, in wireless networks are not fully addressed. It is partially due to the distributed nature of the network and centralized security approaches are sometimes limited or inappropriate. Therefore, it is quite desirable that security schemes can be designed from a node's perspective.

As far as the attacks in wireless networks are concerned, in order to minimize the impact of the attackers, detection mechanisms need to be in place. Therefore, a legitimate/regular node should monitor its surroundings and distinguish a malicious attacker from a regular one. However, the detection process has the following three challenges. (i) monitoring can be costly. To identify the malice, a regular node has to listen to the channel and/or process the information sent by the nodes being monitored. Listening and processing consume resources and hence, monitoring all the times is not efficient even if plausible. (ii) the attacker can camouflage itself. To reduce

the probability of being detected, an attacker can behave like a regular node and choose longer intervals between attacks. (iii) the randomness and unreliability of the wireless channel bring more uncertainty to the monitoring and detection process.

To make the process of detection even more difficult, the attackers do not act passively and wait to be detected. Instead, they also study the interaction they have with the rest of the network and adjust their subsequent actions accordingly. It is also possible that an attacker is wise enough to learn and predict the actions of the regular nodes to assist itself in decision making. The options available to the attackers complicate the solution space and bring more challenges to the detection process.

To model the interaction among the attackers and regular nodes in the network, game theory [4], [11] is introduced as a tool. Recently, game theory has been successfully applied to solve various problems in wireless networks [3], [5], [7], [10], [12], [14]. In the context of attack/intrusion detection, much work has been done that investigates the games played between the regular and attacker nodes. Kodialam *et al.* formally propose a game theoretic framework to model how a service provider detects an intruder [6]. However, their assumptions of zero-sum game and complete, perfect knowledge have limitations. Agah *et al.* study the non-zero-sum intrusion detection game in [1]; their results infer the optimal strategies in one-stage static game with complete information. In [9], Liu *et al.* propose a Bayesian hybrid detection approach to detect intrusion in wireless ad hoc networks. They design an energy efficient detection procedure while improving the overall detection power. The intrusion detection game with networked devices are investigated in [15], where Zhu *et al.* introduce an N-person non-cooperative game to study incentive compatibility of the collaborative detection. [8] models the intention and strategies of a malicious attacker through an incentive-based approach. Cooperative game theory is applied in [2], where Alpcan and Başar model the game as dynamic two-person, non-zero-sum and finite. While existing work focus on various aspects of the detection process, the noise in observation has not been fully addressed.

In this paper we use game theory to capture and analyze the interactions between an attacker and a regular node.

This research was supported by National Science Foundation, under award no. CCF-0950342 and ITT Advanced Engineering & Sciences. Approved for Public Release; distribution unlimited: 88ABW-2009-4436 22 Oct 09.

In particular, we formalize the interactions as a *attacker detection game*, which is a Bayesian game with imperfect information. The information is hidden because the attacker can camouflage as a regular node and the actions are hidden due to the noise and imperfect observation. To address the possible countermeasures the attacker might take, we propose a nested belief model. In this model, the attacker learns from its private observations and predicts if the regular node has accumulated enough information to make the detection. Associated with the belief, we show that a Markov Perfect Bayes-Nash Equilibrium emerges. We also provide simulation study to support the efficiency and other properties of the equilibria.

The rest of the paper is organized as follows. In Section II, we briefly review the basic concepts of game theory that are used in our research. Section III presents the attacker detection game in which we model, analyze and solve some Bayes games in order to obtain equilibrium solutions. Simulation results are shown in Section IV to characterize the equilibrium properties. The last section concludes the paper.

II. BASIC CONCEPTS IN GAME THEORY

Game theory offers powerful tools in modeling and analyzing conflicts and cooperation among multiple players in a system with regard to strategic decision making. In this section, we review some of the fundamental concepts in game theory that will be used and applied throughout this paper. We begin with the definition of games and equilibrium.

DEFINITION 1: A *game* Γ is a tuple (I, S, \mathbf{u}) , where

- $I = 1, 2, \dots, n$ denotes a set of players/nodes.
- $S = \times_{i \in I} S_i$ is a space of strategy profiles. It is the cartesian product of strategy profile S_i for each of the player i .
- \mathbf{u} is a vector of von Neumann-Morgenstern utility functions defined over S . For a particular strategy profile s , $\mathbf{u}(s) = (u_1(s), u_2(s), \dots, u_i(s))$ is called a payoff vector consists of individual payoffs $u_i(s)$.

Often times, player i is interested in what strategies the rest of the players in the game take. We denote the *deleted strategy profile* $s_{-i} = (s_1, \dots, s_{i-1}, s_{i+1}, \dots, s_n)$. We assume that all players in the game are *rational*. A rational player chooses actions to maximize her expected utility (payoffs).

DEFINITION 2: The strategy profile s^* is a Nash Equilibrium, if

$$u_i(s^*) \geq u_i(s_i, s_{-i}^*) \text{ for every strategy } s_i \text{ of player } i.$$

The underlying assumption of Nash Equilibrium is that each player holds the correct belief about other players' actions. However, in many situations, players in the game are not perfectly informed about their opponents' characteristics. This type of games falls into the category of incomplete information games, and the notion of Bayesian game is introduced.

DEFINITION 3: A Bayesian game consists of a set of players and *states*, for each player, a set of *signals* is associated with each of the states. A *belief* about the states is consistent

with the signal. The utility function is defined over the pairs of action and state.

The Perfect Bayes-Nash equilibrium (PBE) is a refinement of Nash Equilibrium in Bayesian games. PBE requires the subsequent plays to be optimal (sequential rationale) and belief system to be consistent for a given strategy profile. In particular, a PBE demands that the belief system $\mu(\theta)$ satisfies the Bayesian conditions [4].

DEFINITION 4: ([4], p331-332) The Bayesian conditions defined for PBE are

B(i): Posterior beliefs are independent. For history $h^{(t)}$, $\mu_i(\theta_{-i}|\theta_i, h^{(t)}) = \prod_{j \neq i} \mu_i(\theta_j|h^{(t)})$.

B(ii): Bayes' rule is used to update beliefs whenever possible.

B(iii): Nodes do not signal what they do not know.

B(iv): Posterior beliefs are consistent for all nodes with a common joint distribution on θ given $h^{(t)}$.

III. ATTACKER DETECTION GAME

A. Game model

To abstract the interactions among the nodes, we consider a two-player game played by the potential attacker node i and the regular node j . This game can be constructed within an application context of packet forwarding [3], [5]. However, the regular node cannot tell if node i is an attacker or not, instead it can only detect the attacker through observations. The process of detecting attackers can be modeled as a Bayesian game. In this game, the types of these nodes, θ_i and θ_j , are private information. While $\theta_j = 0$, i.e., always regular, θ_i can be either 1 (attacker) or 0 (regular), depending on its true type. Since the type of node i is hidden, and the observation is not accurate due to noise and etc., it is a Bayesian game with imperfect information.

The action profiles a_i available to node i are based on its type. For $\theta_i = 0$, $a_i = \{\text{Cooperate}\}$. For $\theta_i = 1$, $a_i \in \{\text{Attack}, \text{Cooperate}\}$, i.e., an attacker can camouflage as regular. Node j has the option to monitor if node i is attacking or not, thus $a_j \in \{\text{Monitor}, \text{Idle}\}$.

To further construct the game, we define the following values. Let u_A be the payoff of a attacker node if it successfully attacks. The cost associated with such an attack is c_A . For the regular node j , the cost of monitoring is u_M and 0 if it is idle. Hence, for the action profile $(a_i, a_j) = (\text{Attack}, \text{Idle})$, the net utility for a successful attacking node i is $u_A - c_A$, the loss for node j is $-u_A$ due to the attack. Similarly, if the action profile is $(a_i, a_j) = (\text{Attack}, \text{Monitor})$, the attacker node i losses $u_A + c_A$, and the net gain for node j is $u_A - u_M$. However, if an attacker node chooses not to attack, the cost to cooperate is u_C . Based on the types of node i and node j , the payoffs matrices are presented in Table I.

In addition, in our model, the channel unreliability implies that monitoring can be accurate with probability $1 - p_e$. We also denote γ as the attack success rate and α as the false alarm rate due to the limitation of the monitoring device.

(a) $\theta_i = 1$, attacker

		Node j			
		Monitor	Idle		
Node i	Attack	$-u_A - c_A$	$u_A - u_M$	$u_A - c_A$	$-u_A$
	Cooperate	$-u_C$	$-u_M$	$-u_C$	0

(b) $\theta_i = 0$, regular

		Node j			
		Monitor	Idle		
Node i	Cooperate	$-u_C$	$-u_M$	$-u_C$	0

TABLE I
PAYOFF MATRIX OF ATTACKER DETECTION GAME.

B. Bayesian games and belief update

Our game analysis is based on the following reasoning. First, it is not efficient for the regular to monitor all times because monitoring is costly, instead, it monitors with a probability. On the other hand, the attacker node does not always attack in order to avoid detection. In the case it is not attacking, it camouflages as a regular node and cannot be identified. When node j is monitoring, it forms a belief about node i on whether it is an attacker or not. This belief is updated over time whenever node i is observed to be an attacker. With the above discussions, we apply Bayes rules to obtain the belief update system for node j . We denote in the $(t+1)^{th}$ stage, q as the monitoring rate, $\Theta = \{0, 1\}$, $\hat{a}_i(t)$ is the observed actions available to node j . The observations are private and subject to noise and error. In particular, we have:

$$\mu_j^{(t+1)}(\theta_i) = \frac{\mu_j^{(t)}(\theta_i)P(\hat{a}_i(t)|\theta_i)}{\sum_{\tilde{\theta}_i \in \Theta} \mu_j^{(t)}(\tilde{\theta}_i)P(\hat{a}_i(t)|\tilde{\theta}_i)}, \quad (1)$$

where $P(\cdot)$ denotes the probability.

For each of the terms in (1), we have the following equations, where A and C denote *Attack* and *Cooperate* respectively.

$$P(\hat{a}_i(t) = A|\theta_i = 1) = p(1 - p_e) + (1 - p)\alpha \quad (2)$$

$$P(\hat{a}_i(t) = A|\theta_i = 0) = \alpha \quad (3)$$

$$P(\hat{a}_i(t) = C|\theta_i = 1) = pp_e + (1 - p)(1 - \alpha) \quad (4)$$

$$P(\hat{a}_i(t) = C|\theta_i = 0) = 1 - \alpha. \quad (5)$$

Since node j does not monitor node i 's actions at every stage, when node j is not monitoring, its belief remains the same at the next stage. Thus, (1) is revised as:

$$\mu_j^{(t+1)}(\theta_i) = q \frac{\mu_j^{(t)}(\theta_i)P(\hat{a}_i(t)|\theta_i)}{\sum_{\tilde{\theta}_i \in \Theta} \mu_j^{(t)}(\tilde{\theta}_i)P(\hat{a}_i(t)|\tilde{\theta}_i)} + (1 - q)\mu_j^{(t)}(\theta_i). \quad (6)$$

With the belief system, the games are played in a sequential manner. As the game evolves, neither nodes can stick to the very same strategy at every stage to yield the most payoffs. Thus, the best response strategies are dependent on the current beliefs held by the nodes. Perfect Bayesian Equilibrium (PBE) can be applied to characterize the aforementioned dependency. In PBE, the belief system is updated by Bayes' rule. PBE also demands that the optimality of subsequent play given the belief. The details of obtaining PBE is presented in [13], and it is not the focus of this paper.

C. Nested belief and Markov Perfect Bayes-Nash Equilibrium

It is natural that not only the regular node but also the attacker node (node i) study the game through observation. In particular, node i understands that although the unreliable channel makes the observations inaccurate, the more often it attacks, the quicker node j can form a correct belief about its attacker type. Thus, node j should take different strategies when different beliefs are held by node j . These strategies are Markovian when we view the beliefs as a set of states. The Markovian strategies adopted by node i is only determined by the current state of the belief, i.e., when the belief update process takes place. However, the belief held by node j is its private information, and by no means can node i access this information. Therefore, it is essential for node i to construct its own belief system, which is the belief on the belief node j holds towards node i and we call this belief developed by node i *nested belief*.

We denote $\mu_i(\mu_j(\theta_i))$ as the nested belief node i holds about node j 's belief about node i , i.e., $\mu_i(\mu_j(\theta_i))$ is the belief about $\mu_j(\theta_i)$. For the game we presented in Table I(a), depending on the actions nodes i and j take, the payoff of node i , u_i , can be one of the three different values: $-u_A - c_A$, $u_A - c_A$ or $-u_C$. While the observations of the payoffs are node i 's private information, given a specific observation o_i , node i can predict the actions taken by node j , despite the prediction may be inaccurate. For example, when $o_i = -u_A - c_A$, node i knows for sure $a_j = \text{Monitor}$. However, when $o_i = -u_C$, node i cannot tell what node i has done. Further, based on the prediction of the actions node j takes, node i can update its belief $\mu_i(\mu_j(\theta_i))$ on how node j 's belief $\mu_j(\theta_i)$ has changed due to a_j . Continuing with the same examples, when $o_i = -u_A - c_A$, $a_j = \text{Monitor}$, so node j observes the *Attack* launched by node i and it will update $\mu_j(\theta_i)$ according to equation 1. Similarly, when $o_i = u_A - c_A$, node i knows that node j is idle and $\mu_j(\theta_i)$ will not change. However, the uncertainty comes when $o_i = -u_C$, where node i cannot accurately update its belief about $\mu_j(\theta_i)$.

To construct the belief update system for node i , we employ the Bayes' Theorem. At stage t of the game, based on the observation $o_i^{(t)}$, node i 's belief $\mu_i(\theta_i)$ is updated as:

$$\mu_i^{(t+1)}(\mu_j(\theta_i)) = \frac{\mu_i^{(t)}(\mu_j(\theta_i))P(o_i^{(t)}|\mu_j(\theta_i))}{\sum_{\tilde{\mu}_j \in \Theta} \mu_i^{(t)}(\tilde{\mu}_j)P(o_i^{(t)}|\tilde{\mu}_j)}, \quad (7)$$

where $\Theta = \{0, 1\}$.

The conditional probabilities of observing o_i given its type θ_i can be calculated as follows. To distinguish from the strategy profiles we used previously, we denote \tilde{p} as the probability node i launches attacks, and \tilde{q} as the probability node j monitors. Therefore, the probabilities that arise due to

the different observations and node i 's type are:

$$P(o_i^{(t)} = -u_A - c_A | \theta_i = 1) = \tilde{p}\tilde{q}(1 - p_e) + (1 - \tilde{p})\tilde{q}\alpha \quad (8)$$

$$P(o_i^{(t)} = -u_A - c_A | \theta_i = 0) = \tilde{q}\alpha \quad (9)$$

$$P(o_i^{(t)} = u_A - c_A | \theta_i = 1) = \tilde{p}[\tilde{q}p_e + (1 - \tilde{q})] \quad (10)$$

$$P(o_i^{(t)} = u_A - c_A | \theta_i = 0) = 0 \quad (11)$$

$$P(o_i^{(t)} = -u_C | \theta_i = 1) = (1 - \tilde{p})[\tilde{q}(1 - \alpha) + (1 - \tilde{q})] \quad (12)$$

$$P(o_i^{(t)} = -u_C | \theta_i = 0) = (1 - \alpha)\tilde{q}. \quad (13)$$

With the above equations, for each of the observations $o_i \in \mathbf{O}$, where $\mathbf{O} = \{-u_A - c_A, u_A - c_A, -u_C\}$, $\mu_i^{(t+1)}(\theta_i)$ is updated independently. Since for the attacker node i , its type $\theta_i = 1$ is known to itself, the overall belief is hence updated considering each of the possible observations.

$$\mu_i^{(t+1)}(\mu_j(\theta_i)) = \sum_{o_i \in \mathbf{O}} P(o_i^{(t)} | 1) \frac{\mu_i^{(t)}(\mu_j(\theta_i)) P(o_i^{(t)} | \theta_i)}{\sum_{\tilde{\theta}_i \in \Theta} \mu_i^{(t)}(\mu_j(\tilde{\theta}_i)) P(o_i^{(t)} | \tilde{\theta}_i)}. \quad (14)$$

Further, with the belief system of node i , the attacker detection game can be solved obtain the sequential rationality. Moreover, it is justified that the belief update process for node i also satisfies the Bayesian condition in Definition 4. The reasons are: B(i) is satisfied because $\theta_j = 0$ all the time. Equation (7) is derived from Bayes' rule, and hence B(ii) is also satisfied. B(iii) is fulfilled because node i 's observed signals is determined by its actions. B(iv) is trivial in our game because no third player exists. In addition, equation (15) suggests that node i 's strategy is purely dependent on the current belief it holds. Thus, we can further refine the PBE in attacker detection game.

Solving the game, we get a Markov Perfect Bayes-Nash Equilibrium (MPBNE), with the equilibrium profile as in the following theorem.

THEOREM 1: The attacker detection game has a MPBNE for subgame stage k when

$$\tilde{p}^{(k)} = \frac{u_M}{\mu_i^{(k)}(\mu_j(\theta_i = 1))u_A(1 + \gamma)(1 - p_e)} \quad (15)$$

$$\tilde{q}^{(k)} = \frac{u_A\gamma - c_A + u_C}{u_A(1 - p_e)(1 + \gamma)}. \quad (16)$$

Proof: Please refer to the Appendix ■

A special case for the strategy profile σ_i is "Always attack when $\mu_i^{(k)}(\mu_j(\theta_i = 1)) < \bar{\mu}$ and cooperate otherwise, for a predefined threshold $\bar{\mu} \in (0, 1)$ ". In this strategy, when $\mu_i^{(k)}(\mu_j(\theta_i = 1)) < \bar{\mu}$, $\tilde{p} = 1$ and node j will progressively update its belief when it monitors because node i is always behaving maliciously. However, when the belief threshold is reached, node i will refrain from launching attacks, and hence its payoff will decrease. It is clear that the strategy deviates from the MPBNE because \tilde{p} does not adhere to the equilibrium. As a result, node i will be identified quickly and it will be dormant for the rest of the time. While this strategy is favorable to node j and the network, from node i 's perspective, this strategy will limit its attacks and hence it is not desirable.

IV. SIMULATION

We study the characteristics of the Markov Perfect Bayes-Nash Equilibrium. In particular, we are interested in the properties of node i 's belief update system (i.e., nested belief) and how the results would differ from that without node i 's belief. It is noted that for node j 's belief system, a complete study can be found in [13].

In Figure 1, we study node i 's belief system in the MPBNE. The plots are obtained with $p_e = 0.01$, $\gamma = 0.95$ and $\alpha = 0.05$. To better show the properties of node i 's belief system in the MPBNE, we also present node j 's belief system. In particular, we plot μ_i as node i 's belief system in MPBNE according to equation (14), μ_j as node j 's belief system in PBE as stated in equation (6) and μ_j^* as node j 's belief system update in the MPBNE as a result of node i 's actions in the nested belief model. A common observation is that node i 's belief μ_i converges much faster than the belief μ_j in PBE, which means that node i holds a false belief that node j can identify its malice quicker than node j actually could. As a result of the inaccuracy in node i 's belief, it takes longer time for node j to form a belief on node i . This is evident from the plots that show μ_j^* converges much slowly than it does in PBE, when node i does not employ any belief system.

In addition, Figure 1(b) indicates a larger detection gain will force node i 's belief system converge quicker. Figures 1(c) and 1(d) infer that reliable channel, high attack success rate and accurate detection (low false alarm rate) will also induce a fast convergence of μ_i . Moreover, a high disguise cost helps μ_i converge faster. The reason lies in the inaccuracy of node i 's belief system. From our previous discussion, it is stated that when the observed payoff is $-u_C$, node i cannot predict what node j 's action is. Thus, an internal error resides in node i 's belief system, and this error is amplified when u_C is large (i.e., u_C takes a high weight in the payoff), which corresponds to a large disguise cost.

The properties of the MPBNE strategy are further investigated in Figure 2. Both the MPBNE strategy attack probability, denoted as p_M and the PBE strategy attack probability will increase with smaller attack gain and attack success rate, as well as larger channel error rate and false alarm rate. Moreover, it is noted that p_M is smaller than what node j believes it would be (denoted as p_{j*i} in the Figures 2(a)). In addition, p_M is larger than the PBE strategy attack probability p_{PBE} in the first several stage games, however, as the games repeat, p_M drops below p_{PBE} . This interesting observation implies that when node i implements the belief system, it attacks more aggressively (than without the belief about belief model, i.e., in PBE) in the first several games, because it believes node j is far from reaching a successful detection. As the game unfolds, node i adjusts its attack rate to prevent from detection. The difference between p_M and p_{PBE} also explains why node j 's belief system alters in the MPBNE as shown in Figure 1.

V. CONCLUSIONS

In this paper, we apply game theory to study attacker detection in wireless networks with lossy channels. We formulate an

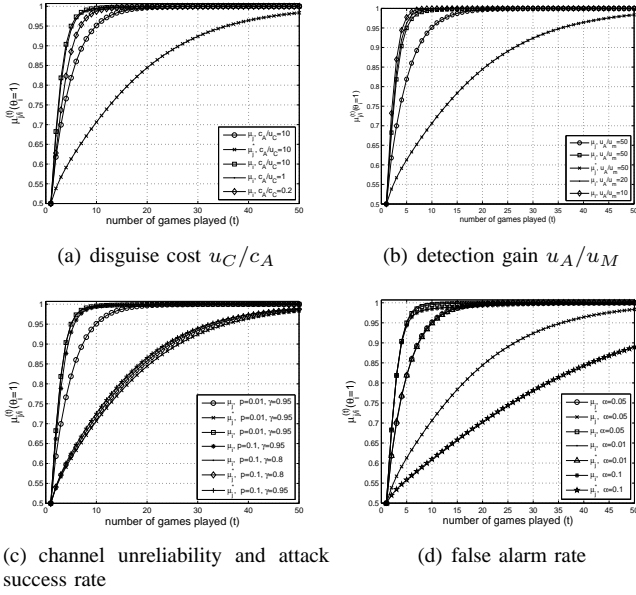


Fig. 1. Node i 's belief system update in the Markov Perfect Bayes-Nash Equilibrium.

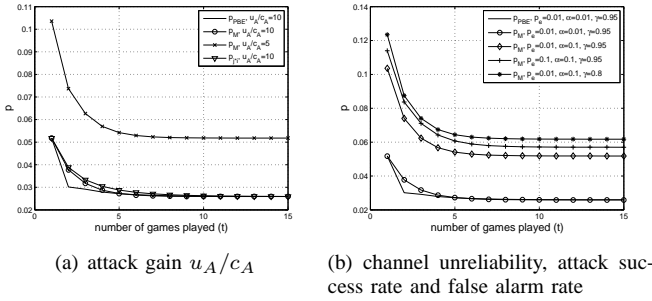


Fig. 2. Effect of parameters on the Markov Perfect Bayes-Nash Equilibrium strategy.

attacker detection game and apply Bayes analysis to obtain the equilibria with imperfect information. We introduce the nested belief model as countermeasures available to the attackers. MPBNE is derived and it postpone the detection of attackers. Simulations are provided to illustrate the properties of the equilibrium in terms of disguise cost, attack success rate, detection gain, attack gain, channel loss, and false alarm rate.

REFERENCES

- [1] A. Agah, S. K. Das, K. Basu and M. Asadi, "Intrusion detection in sensor networks: A non-cooperative game approach", *Proceedings of IEEE NCA 2004*, pp. 343-346.
- [2] T. Alpcan and T. Başar, "Game theoretic approach to decision and analysis in network intrusion detection", *Proceedings of IEEE CDC 2003*.
- [3] L. Buttyán and J. P. Hubaux, "Stimulating cooperation in self-organizing mobile ad-hoc networks", *ACM/Kluwer Mobile Networks and Applications*, 8(5), pp. 579-592.
- [4] D. Fudenberg and J. Tirole, *Game Theory*, MIT press, Cambridge, MA, 1991.
- [5] J. J. Jaramillo and R. Srikant, "DARWIN: distributed and adaptive reputation mechanism for wireless ad-hoc networks", *Proceedings of ACM MobiCom 2007*, pp. 87-97.
- [6] M. Kodialam and T. V. Lakshman, "Detecting network intrusion via sampling: a game theoretic approach", *Proceedings of IEEE Infocom 2003*, pp. 1880-1889.

- [7] X. -Y. Li, Y. Wu, P. Xu, G. Chen and M. Li, "Hidden Information and Actions in Multi-Hop Wireless Ad Hoc Networks", *Proceedings of ACM Mobihoc 2008*, pp. 283-292.
- [8] P. Liu, W. Zhang and M. Yu, "Incentive-based modeling and inference of attacker intent, objectives, and strategies", *ACM Trans. on Information and System Security*, 56(3), pp. 78-118, 2005.
- [9] Y. Liu, C. Comaniciu and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks", *Proceedings of ACM GameNets 2006*.
- [10] A. B. Mackenzie and L. A. DaSilva, *Game Theory for Wireless Engineers*, San Rafael, California: Morgan & Claypool Publishers, 2006.
- [11] M. J. Osborne, "An introduction to Game Theory", *Oxford University Press*, New York, NY, 2004.
- [12] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao, "Cooperation in wireless ad hoc networks", *Proceedings of IEEE Infocom 2003*, pp. 807-817.
- [13] W. Wang, M. Chatterjee and K. Kwiat, "Coexistence with Malicious Nodes: A Game Theoretic Approach.", *Proceedings of GameNets 2009*, pp. 277-286.
- [14] J. Zhang and Q. Zhang, "Stackelberg Game for Utility-Based Cooperative Cognitive Radio Networks", *Proceedings of ACM Mobihoc 2009*, pp. 23-32.
- [15] Q. Zhu, C. Fung, R. Boutaba and T. Başar, "A Game-Theoretical Approach to Incentive Design in Collaborative Intrusion Detection Networks", *Proceedings of GameNets 2009*, pp. 384-392.

APPENDIX

THEOREM 1: The attacker detection game has a MPBNE for subgame stage k when

$$\begin{aligned}\tilde{p}^{(k)} &= \frac{u_M}{\mu_i^{(k)}(\mu_j(\theta_i = 1))u_A(1 + \gamma)(1 - p_e)} \\ \tilde{q}^{(k)} &= \frac{u_A\gamma - c_A + u_C}{u_A(1 - p_e)(1 + \gamma)}.\end{aligned}$$

Proof: Consider at an arbitrary stage k of the game, the equilibrium point infers indifference, which means $u_i^{(k)}(Attack) = u_i^{(k)}(Cooperate)$ and $u_j^{(k)}(Monitor) = u_j^{(k)}(Idle)$. In particular,

$$\begin{aligned}u_i^{(k)}(a_i^{(k)} = Attack|a_j^{(k)} = Monitor) = \\ -(u_A + c_A)(1 - p_e)\tilde{q}^{(k)} + (u_A - c_A)\gamma(1 - \tilde{q}^{(k)}) \\ + (u_A - c_A)\gamma\tilde{q}^{(k)}p_e - c_A(1 - \gamma)p_e\tilde{q}^{(k)} \\ - c_A(1 - \tilde{q}^{(k)})(1 - \gamma)\end{aligned}\quad (17)$$

$$u_i^{(k)}(a_i^{(k)} = Cooperate|a_j^{(k)} = Monitor) = -u_C. \quad (18)$$

$$\begin{aligned}u_j^{(k)}(a_j^{(k)} = Monitor|a_i^{(k)} = Attack) = \\ \mu_i(\mu_j^{(k)}(\theta_i = 1))\tilde{p}^{(k)}[\gamma(u_A - u_M)(1 - p_e) \\ + (1 - \gamma)(1 - p_e)(u_A - u_M) - (1 - \gamma)p_e u_M \\ - \gamma p_e(u_A + u_M)] - (1 - \tilde{p}^{(k)})\mu_i(\mu_j^{(k)}(\theta_i = 1))u_M \\ \mu_i(\mu_j^{(k)}(\theta_i = 0))u_M\end{aligned}\quad (19)$$

$$\begin{aligned}u_j^{(k)}(a_j^{(k)} = Idle|a_i^{(k)} = Attack) = \\ -\tilde{p}^{(k)}u_A\gamma\mu_i(\mu_j^{(k)}(\theta_i = 1)).\end{aligned}\quad (20)$$

The solutions to the above equations are the $\tilde{p}^{(k)}$ and $\tilde{q}^{(k)}$ values in the theorem, which indicate the sequential rationality. In addition, our discussion of the nested belief shows that node i 's belief update satisfies the Bayesian conditions. Thus, $\tilde{p}^{(k)}$ and $\tilde{q}^{(k)}$ are the MPBNE solution to the attacker detection game. ■